UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/783,859	02/19/2004	Lawrence A. Spracklen	SUNMP501	7656

32291 7590 05/19/2008
MARTINE PENILLA & GENCARELLA, LLP
710 LAKEWAY DRIVE
SUITE 200
SUNNYVALE, CA 94085

EXAMINER	
TOLENTINO, RODERICK	
ART UNIT	PAPER NUMBER
2134	
MAIL DATE	DELIVERY MODE
05/19/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/783,859	SPRACKLEN, LAWRENCE A.	
	Examiner	Art Unit	
	Roderick Tolentino	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03/17/2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9,12,13,15 and 17-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1–9, 12, 13, 15 and 17–19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *19 February 2004* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1 – 9, 12, 13, 15 and 17 – 19 are pending.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 03/17/2008 has been entered.

Response to Arguments

3. Applicant's arguments with respect to claim1, 7, 12 and 17 have been considered but are moot in view of the new ground(s) of rejection, as necessitated by amendment filed 03/17/2008.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1 – 3, 7, 12, 17 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Black et al. U.S. Patent No. (7,103,602) in view of Col et al. U.S. Patent No. (6,330,657), Oka et al. U.S. PG-Publication No. (2002/0108042) and O'Gorman et al. U.S. PG-Publication No. (2003/0061548).

6. As per claims 1, 7, 12 and 17, Black teaches a processor capable of executing a secure hash algorithm (SHA) (Black, Col. 2 Lines 14 – 30, processor that can compute SHA), but fails to teach the first execution unit defined to communicate a partial result of the schedule computation on the data block to the second execution unit when the partial result becomes available and prior to completion of the schedule computation on the data block, wherein the second execution unit is defined to perform a compression function on the partial result received from the first execution unit in parallel with the first execution unit continuing the schedule computation on the data block and wherein an output, of the first execution unit is connected to an input of the second execution unit. However, in an analogous art Col teaches the first execution unit defined to communicate a partial result of the schedule computation on the data block to the second execution unit when the partial result becomes available and second execution in parallel with the first execution unit continuing the schedule computation on the data block (Col, Col.14 Lines 1 – 20, parallel processing execution) and Oka teaches prior to completion of the schedule computation on the data block, wherein the second execution unit is defined to perform a compression function on the partial result received from the first execution unit (Oka, Paragraph 0153, Compressing function) and O'Gorman teaches wherein an output, of the first execution unit is connected to an input

of the second execution unit (O'Gorman, Paragraph 0024, First output becomes an input for a second execution).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Col's pairing of microinstructions in the instruction queue with Black's system for data management, because it offers the advantage of being efficient in the execution of instructions (Col, Col. 1 Lines 43 – 50).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Oka's public key certificate issuing system with Black's system for data management, because it offers the advantage of securing data security (Oak, Paragraph 0003).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use O'Gorman's method for verifying the integrity of control module operation with Black's system for data management, because it offers the advantage of not requiring the execution of redundant algorithms (O'Gorman, Paragraph 0006).

7. As per claims 2, Black as modified teaches wherein the first execution unit is a single instruction multiple data (SIMD) execution unit (Col, Col. 3 Lines 61 – 63).

8. As per claim 3, Black as modified teaches the second execution unit is an integer execution unit (Col, Col. 14 Lines 10 – 16).

9. As per claim 19, Black as modified teaches operating the second execution unit to perform the compression function includes rotating bits in the partial result (Oka, Paragraph 0153, Compressing function).

10. Claims 4, 5, 8 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Black et al. U.S. Patent No. (7,103,602), Col et al. U.S. Patent No. (6,330,657),Oka et al. U.S. PG-Publication No. (2002/0108042) and O'Gorman et al. U.S. PG-Publication No. (2003/0061548), as applied to claim 1 and in further view of Lilly U.S. Patent No. (6,829,355).

11. As per claim 4, Black fails to teach wherein the message is a parsed padded message. However, in an analogous art Lilly teaches the message is a parsed padded message (Lily, Col. 3 Lines 32 – 38).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Lilly's device for one-way hashing with Black's system for data management, because it offers the advantage of to maintain and improve security (Lilly, Col. 2 Lines 10 – 13).

12. As per claim 5, Black as modified teaches the parsed padded message includes an original message and a plurality of pad bits, the original message being a plurality of bits (Lilly, Col. 3 Lines 32 – 38).

13. As per claim 8, Black fails to teach the first execution unit receives a plurality of blocks, the plurality of blocks including an original message and a plurality of pad bits. However, in an analogous art Lilly teaches the first execution unit receives a plurality of blocks, the plurality of blocks including an original message and a plurality of pad bits (Lilly, Col. 3 Lines 5 – 10).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Lilly's device for one-way hashing with Black's system for data management, because it offers the advantage of to maintain and improve security (Lilly, Col. 2 Lines 10 – 13).

14. As per claim 13, Black as modified teaches the cryptographic computation is further capable of performing a preprocessing operation (Col, Col. 20 Lines 45 – 54) but fails to teach the preprocessing operation includes padding the message, parsing a padded message and setting initial hash values. However, in an analogous art Lilly teaches the preprocessing operation includes padding the message, parsing a padded message and setting initial hash values (Lily, Col. 3 Lines 32 – 38).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Lilly's device for one-way hashing with Black's system for data management, because it offers the advantage of to maintain and improve security (Lilly, Col. 2 Lines 10 – 13).

15. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Black et al. U.S. Patent No. (7,103,602), Col et al. U.S. Patent No. (6,330,657), Oka et al. U.S. PG-Publication No. (2002/0108042) and O'Gorman et al. U.S. PG-Publication No. (2003/0061548) and in further view Tague et al. U.S. Patent No. (4,799,181).

16. As per claim 6, Black fails to teach the partial result includes a group of bits capable of being represented by a hexadecimal value. However, in an analogous art

Tague teaches the partial result includes a group of bits capable of being represented by a hexadecimal value (Tague, Col. 1 Lines 52 – 57).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Tague's BCD arithmetic using binary arithmetic and logical operations with Black's system for data management, because it offers the advantage of to being a more efficient way of processing data (Tague, Col. 1 Lines 25 – 29).

17. Claims 9, 15 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Black et al. U.S. Patent No. (7,103,602), Col et al. U.S. Patent No. (6,330,657), Oka et al. U.S. PG-Publication No. (2002/0108042), O'Gorman et al. U.S. PG-Publication No. (2003/0061548) and Lilly U.S. Patent No. (6,829,355), and in further view Gibson U.S. Patent No. (5,155,820).

18. As per claims 9, 15 and 18, Black fails to teach message schedule computation includes a rotation operation capable of rotating the plurality of blocks. In an analogous art Gibson teaches message schedule computation includes a rotation operation capable of rotating the plurality of blocks (Gibson, Col. 9 Lines 7 – 27).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Gibson's instruction format with designation for operand lengths with Black's system for data management, because it offers the advantage of processing very fast while at a low cost (Gibson, Col. 3 Lines 23 – 28).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Roderick Tolentino whose telephone number is (571) 272-2661. The examiner can normally be reached on Monday - Friday 9am to 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Roderick Tolentino
Examiner
Art Unit 2134

Roderick Tolentino

/R. T./

Examiner, Art Unit 2134

/Benjamin E Lanier/
Primary Examiner, Art Unit 2132